JOURNAL OF COMBINATORIAL THEORY (A) 15, 333–337 (1973)

Note

On the MacWilliams Identity

NEAL ZIERLER

Institute for Defense Analyses, Princeton, New Jersey 08540

Communicated by Marshall Hall, Jr.

Received February 8, 1972

A generalization of the MacWilliams relation between the Hamming weight distributions in a linear subspace of a vector space over a finite field and its dual is deduced from an observation concerning the Fourier transforms of certain members of the group algebra of the additive group of the space.

I wish to thank R. J. McEliece for sending me a proof of the lemma of this note attributed to A. M. Gleason, which I have used in place of my original and more complicated one, and for communicating the application of our theorem made by Howard Rumsey, Jr., which now appears here as the corollary. Gleason's proof and related material of interest appeared in a privately circulated memorandum by E. F. Assmus, Jr., H. F. Mattson, Jr. and R. J. Turyn.

Let p be a prime, m and n positive integers, $q = p^m$ and $V^n = (\mathrm{GF}(q))^n$, the Cartesian product of n copies of a field with q elements. For u and v in V^n let $[u, v] = \sum u_i v_i$ in $\mathrm{GF}(q)$. A norm for V^n is defined by setting $| u |$ equal to the number of non-zero values of the list u. In the theory of error-correcting codes, it is customary to call $| u |$ the Hamming weight of u. For $A \subset V^n$, let $A^\perp = \{u \in V^n \,|\, [u, v] = 0 \text{ for all } v \in A\}$. Let $N(A, i)$ be the number of elements v in A such that $| v | = i$. Now let x be an indeterminate over the reals, let k be a positive integer at most n and let A be a $\mathrm{GF}(q)$-linear subspace of V^n of dimension k. The following relation, discovered by J. MacWilliams [2], has important applications in the theory of error-correcting codes (see [1]).

$$\sum_{i=0}^{n} N(A, i)(1 - x)^i (1 + (q - 1)x)^{n-i} = q^k \sum_{i=0}^{n} N(A^\perp, i)\, x^i. \qquad (1)$$

Let $f: \mathrm{GF}(q) \to \mathrm{GF}(p)$ be an epimorphism of additive groups. For

$u, v \in V^n \times V^n$, let $(u, v) = f[u, v]$. Clearly $(-, -)$ is a non-degenerate symmetric GF(p)-bilinear form. Let ω be a primitive p-th root of unity. For u in V^n define the function $\chi_u : V^n \to C$ (the complex numbers) by

$$\chi_u(v) = \omega^{(u,v)}. \tag{2}$$

It is easy to see that $u \mapsto \chi_u$ is an isomorphism of the additive group V^n to its dual $\hat{V}^n$ that is symmetric in the sense that $\chi_u(v) = \chi_v(u)$.

Now let A be a family of elements of V^n; that is, a collection in which each element may appear any finite number of times. Accordingly, we let $N(A, i)$ denote the number of appearances in A of elements of weight i, including repetitions. Our main objective is to prove the following theorem which, in effect, transforms algebraic constraints on a family A into constraints among the numbers $N(A, i)$.

THEOREM. *Let A be a family of elements of V^n. Then*

$$\sum_{i=0}^{n} N(A, i)(1 - x)^i (1 + (q - 1)x)^{n-i} = \sum_{v \in V^n} x^{|v|} \sum_{u \in A} \chi_v(u). \tag{3}$$

Although the isomorphism $v \mapsto \chi_v$ depends on the choice of the epimorphism f: GF(q) $\to$ GF(p), the polynomial appearing on the right side of (3) does not. This is a consequence of the theorem, since the left side is independent of f. It also follows directly from the observation that the set of elements of V^n of norm i is closed under multiplication by the non-zero elements of GF(q).

Applying the theorem in the case that $A = w + B$ where $w \in V^n$ and B is a GF(q)-subspace of V^n of dimension k, we have

$$\sum_{u \in A} \chi_v(u) = \sum_{u \in B} \chi_v(w + u) = \chi_v(w) \sum_{u \in B} \chi_v(u).$$

The restriction of χ_v to B is a character of B, so the sum is 0 unless $\chi_v \equiv 1$ on B and this occurs just when $v \in B^\perp$. Hence (3) becomes

$$\sum_{i=0}^{n} N(A, i)(1 - x)^i (1 + (q - 1)x)^{n-i} = q^k \sum_{v \in B^\perp} x^{|v|} \chi_w(v). \tag{4}$$

If $w \in B$, that is, if A is a subspace, $\chi_w \equiv 1$ on $A^\perp = B^\perp$ and (4) reduces to (1).

In coding theory, it is the distance spectrum of a code rather than the weight spectrum that is of interest. Thus let C be any (linear or nonlinear) code of length n over GF(q)—that is, any subset of V^n—and let A be the

family (with repetitions) of all $c - c'$ for $c, c' \in C$. Applying the theorem,

$$\sum_{i=0}^{n} N(A, i)(1 - x)^i (1 + (q - 1)x)^{n-i} = \sum_{v \in V^n} x^{|v|} \sum_{c, c' \in C} \chi_v(c - c')$$

$$= \sum_{v \in V^n} x^{|v|} \left| \sum_{c \in C} \chi_v(c) \right|^2.$$

Let $a_i = N(A, i)/|\ C\ |^2$, the probability that two code words chosen at random (uniformly) are separated by i, and let

$$b_i = \sum_{|v|=i} \left| \frac{1}{|\ C\ |} \sum_{c \in C} \chi_v(c) \right|^2.$$

We have:

COROLLARY.

$$\sum_{i=0}^{n} a_i(1 - x)^i (1 + (q - 1)x)^{n-i} = \sum_{i=0}^{n} b_i x^i.$$

Note that $0 \leqslant b_i \leqslant \sum_{|v|=i} 1 = \binom{n}{i}(q - 1)^i$ and that, if the code is linear, b_i can be interpreted as the number of words of weight i in the dual code.

Let $H = C^{V^n}$ with the inner product

$$\alpha, \beta \mapsto \sum_{u \in V^n} \alpha(u)\, \bar{\beta}(u).$$

The normalized characters $\{q^{-n/2}\chi_u \mid u \in V^n\}$ form an orthonormal basis for H. For each α in H we define $\hat{\alpha}$ in H by

$$\hat{\alpha}(u) = q^{-n/2} \sum_{v \in V^n} \alpha(v)\, \bar{\chi}_u(v). \tag{5}$$

The function $\alpha \mapsto \hat{\alpha}$ is an involution (= involutory isometry) of H.

For each real number b define the member β_b of H by $\beta_b(v) = b^{|v|}$.

LEMMA. $\hat{\beta}_b(u) = q^{-n/2}(1 - b)^{|u|}(1 + (q - 1)\, b)^{n-|u|}$.

Proof. For $a \in \mathrm{GF}(q) = V^1$, $|\ a\ |$ = rational 0 if $a = 0$, = rational 1 otherwise. Now

$$q^{n/2}\hat{\beta}_b(u) = \sum_{v} b^{|v|} \bar{\omega}^{(u,v)}$$

$$= \sum_{v} b^{|v_1| + \cdots + |v_n|} \bar{\omega}^{f(u_1 v_1) + \cdots + f(u_n v_n)}$$

$$= \prod_{i=1}^{n} \sum_{v_i \in \mathrm{GF}(q)} b^{|v_i|} \bar{\omega}^{f(u_i v_i)}.$$

If $u_i = 0$, the sum is

$$\sum_{v_i} b^{|v_i|} = 1 + (q-1)b.$$

If $u_i \neq 0$, the sum is

$$\begin{aligned} &1 + b \sum_{v_i \neq 0} \bar{\omega}^{f(u_i v_i)} \\ &\quad = 1 + b \sum_{v_i \neq 0} \bar{\omega}^{f(v_i)} \\ &\quad = 1 + b((1 + \omega + \omega^2 + \cdots + \omega^{p-1})q/p + \omega + \omega^2 + \cdots + \omega^{p-1}) \\ &\quad = 1 - b, \end{aligned}$$

since $1 + \omega + \omega^2 + \cdots + \omega^{p-1} = 0$. Hence the product is $(1-b)^{|u|} \times (1 + (q-1)b)^{n-|u|}$, and the lemma is proved.

The theorem follows from the lemma simply by summing both sides over all u in the given family A, when $\hat{\beta}_b(u)$ is replaced by its defining sum (5). This proves that the polynomial relation (3) holds for infinitely many values $x = b$, and hence it holds for the indeterminate x as well.

For what isomorphisms χ of V^n to $\hat{V}^n$ do the foregoing results hold? Let ω and f be as before a primitive complex p-th root of 1 and an epimorphism of GF(q) to GF(p), respectively. It is not difficult to show that the function $\alpha \mapsto \hat{\alpha}$ induced by an isomorphism $\chi : V^n \to \hat{V}^n$, $u \mapsto \chi_u$ via (5) is an involution of H if and only if

$$\chi_u(v) = \omega^{f[Tu,Tv]},$$

where T is an automorphism of the additive group V^n. It may further be shown that the lemma, or, equivalently, the theorem, holds for the function $\alpha \mapsto \hat{\alpha}$ if and only if T has the additional property: $|Tu| = |u|$ for all u in V^n. Finally, in order to deduce (1) from the theorem, T must also satisfy: $[u, v] = 0$ implies $[Tu, Tv] = 0$. Then it follows easily that the possible choices of χ are just

$$\chi_u(v) = \omega^{g[u,v]}$$

where g is any epimorphism of GF(q) to GF(p).

In the application to error-correcting codes, the additive group of GF(q) is usually given concretely as $(\mathrm{GF}(p))^m$. In this case each value u_i of a list u in V^n is itself a list of elements of GF(p). One then has the natural epimorphism

$$f_0 : u_i \mapsto \sum_{j=1}^{m} u_{ij},$$

and hence the canonical identification χ of V^n with

$$\hat{V}^n: u \mapsto \chi_u, \qquad \chi_u(v) = \omega^{r_0[u,v]}.$$

REFERENCES

1. BERLEKAMP, E. R., "Algebraic Coding Theory," McGraw-Hill, New York, 1968.
2. MACWILLIAMS, J., A theorem on the distribution of weights in a systematic code, *Bell System Tech. J.* **42** (1963), 79–84.